Cryptography and Communications (2022) 14:1081–1089
https://doi.org/10.1007/s12095-022-00577-4

A note on the differential spectrum of a class of power mappings with Niho exponent

Haode Yan[1] · **Zhen Li**[1]

Received: 23 September 2021 / Accepted: 24 March 2022 / Published online: 7 April 2022

Abstract

Let $\mathrm{GF}(q^2)$ be the finite field containing q^2 elements, where q is an odd prime power. In this paper, we study the differential properties of the power mapping $F(x)=x^d$ over $\mathrm{GF}(q^2)$, where $d=2q-1$ is a Niho exponent [14]. The differential spectrum of F is given by $\mathbb{S}=\{\omega_0=\frac{q^2+q-2}{2},\omega_2=\frac{q^2-q}{2},\omega_q=1\}\cdot$

Keywords Power mapping · Differential uniformity · Differential spectrum · Niho exponent

Mathematics Subject Classification (2010) 11T06 · 94A60

1 Introduction

Let $\mathrm{GF}(q)$ be the finite field with q elements, where q is a prime power. For any function $f:\mathrm{GF}(q)\rightarrow\mathrm{GF}(q)$, the *derivative* of f in respect to any given $a\in\mathrm{GF}(q)$ is a function from $\mathrm{GF}(q)$ to $\mathrm{GF}(q)$ defined by

$$D_a f(x)=f(x+a)-f(x),\forall x\in\mathrm{GF}(q).$$

For any $b\in\mathrm{GF}(q)$ and $a\in\mathrm{GF}(q)^*:=\mathrm{GF}(q)\backslash\{0\}$, we denote

$$\delta(a,b)=\#\{x\in\mathrm{GF}(q)\mid D_af(x)=b\}.$$

The *differential uniformity* of f is defined as

$$\delta=\max_{a\in\mathrm{GF}(q)^*,\,b\in\mathrm{GF}(q)}\delta(a,b),$$

and f is said to be *differentially δ-uniform* [15]. Differential uniformity is an important concept in cryptography since it quantifies the degree of security of a Substitution box

✉ Haode Yan
hdyan@swjtu.edu.cn

Zhen Li
lz-math@my.swjtu.edu.cn

[1] School of Mathematics, Southwest Jiaotong University, Chengdu 610031, China

(S-box) used in the cipher with respect to differential attacks [1]. Clearly, $\delta \geq 1$ for any f over GF(q). In particular, a function f with the lowest differential uniformity $\delta = 1$ is called a perfect nonlinear (PN) function, which only exists in odd characteristic finite fields. Functions with differential uniformity $\delta = 2$ are called almost perfect nonlinear (APN) functions, which have the lowest differential uniformity over even characteristic finite fields. For more information on PN and APN functions, the readers are referred to [5] and [6].

Power functions with low differential uniformity serve as good candidates for the design of S-boxes not only because of their strong resistance to differential attacks but also for the usually low implementation cost in hardware. Therefore, it is worthy to study power functions with low differential uniformity. When $f(x) = x^d$ is a power function over GF(q), it is easy to see that $\delta(a, b) = \delta\left(1, \frac{b}{a^d}\right)$ for any $a \in \mathrm{GF}(q)^*$. This implies that the differential properties of f are completely determined by the values of $\delta(1, b)$ when b runs through GF(q). In [2], the *differential spectrum* of a power function is defined as follows.

Definition 1 [2] Let $f(x) = x^d$ be a power function over GF(q) with differential uniformity δ. Denote

$$\omega_i = \#\{b \in \mathrm{GF}(q) \mid \delta(1, b) = i\},$$

where $0 \leq i \leq \delta$. The differential spectrum of f is defined to be the multiset

$$\mathbb{S} = \{\omega_i \mid 0 \leq i \leq \delta\}.$$

Sometimes the zeros in $\mathbb{S}$ can be omitted. The differential spectrum of f over GF(q) satisfies the following identities (see [2]).

$$\sum_{i=0}^{\delta} \omega_i = \sum_{i=0}^{\delta} i\omega_i = q. \tag{1}$$

The identities (1) are useful in computing the differential spectrum of f. From (1), it is easy to see that all PN functions over GF(q) have the same differential spectrum $\mathbb{S} = \{\omega_1 = q\}$, and all APN functions over GF(2^n) have the same differential spectrum $\mathbb{S} = \{\omega_0 = 2^{n-1}, \omega_2 = 2^{n-1}\}$. Moreover, we have the following relationship between the differential spectrum and the number of solutions of a system of equations with four variables.

Lemma 1 [11] With the notation introduced in Definition 1, let N_4 denote the number of solutions $(x_1, x_2, x_3, x_4) \in (\mathrm{GF}(q))^4$ of the system of equations

$$\begin{cases} x_1 - x_2 + x_3 - x_4 = 0, \\ x_1^d - x_2^d + x_3^d - x_4^d = 0. \end{cases}$$

Then we have

$$\sum_{i=0}^{\delta} i^2\omega_i = \frac{N_4 - q^2}{q - 1}.$$

As pointed out in [2], the differential spectrum of S-boxes is useful to analyze the resistance of the cipher to the differential attacks and to its variations. For example, the inverse function x^{-1} over GF(2^n) with even n has the best resistance to differential cryptanalysis for 4-uniform S-boxes, since it has the differential spectrum $\mathbb{S} = \{\omega_0 = 2^{n-1} + 1, \omega_2 = 2^{n-1} - 2, \omega_4 = 1\}$. However, it seems difficult to determine the differential spectrum of a power function. Only a few power mappings over GF(2^n) have known differential spectrum, the readers are referred to [2–4, 17, 18]. For the power mappings over odd characteristic finite fields, the known results are introduced as follows. Dobbertin et al. determined the differential spectrum of the ternary Welch power mapping $x^{2\cdot 3^{\frac{n-1}{2}}+1}$ over GF(3^n) with odd n, which was used in the study of the cross-correlation function of an m-sequence and its decimated sequence [9]. In [7], Choi et al. computed the differential spectra of two classes of power mappings. The differential spectrum of p-ary Kasami power function was studied in [21] and [12]. Recently, the differential spectrum of x^{p^n-3} over GF(p^n) was determined in [16] and [20]. Yan and Li investigated the differential spectrum of $x^{\frac{5^n-3}{2}}$ over GF(5^n), which was an involution function with algebraic degree n [19]. We summarize the known results in Table 1. By the main result in [8], the power mappings in Table 1 are pairwise CCZ-inequivalent.

Niho exponents were introduced by Yoji Niho, who investigated the cross-correlation function between an m-sequence and its decimation sequence in 1972 [14]. Since then, Niho exponents have been widely used in other research areas such as cryptography and coding theory. For the recent progress in the application of Niho exponents, the readers are referred to [13]. We focus on the power mapping $F(x) = x^{2q-1}$ over GF(q^2), where q is an prime power. Herein $2q - 1$ is a Niho exponent. This exponent was first studied by Niho in [14]. which was used to construct m-sequences with four-valued cross-correlation function. Helleseth found the distribution of the cross-correlation function when $q \not\equiv 2 (\mathrm{mod}\ 3)$ [10]. When q is a power of 2, the differential spectrum of F was computed by Blondeau et al. in 2011. It is rational to consider the differential spectrum of F for the case that q is an odd prime power. In this paper, we mainly study the differential spectrum of $F(x) = x^{2q-1}$ over GF(q^2), where q is an odd prime power. By solving certain differential equations over finite fields, we determine the differential spectrum of F in Section 2. The number of solutions of a system of equations with four variables is obtained from the differential spectrum. Section 3 concludes this paper.

Table 1 Power mappings x^d over GF(p^n) with known differential spectrum (p is odd)

p	d	Conditions	Differential uniformity	Reference
3	$2\cdot 3^{\frac{n-1}{2}}+1$	n is odd	4	[9]
odd	$\frac{p^k+1}{2}$	$e = \gcd(n,k)$	$\frac{p^e-1}{2}$ or p^e+1	[7]
odd	$\frac{p^n+1}{p^m+1} + \frac{p^n-1}{2}$	$p^n \equiv 3 \pmod 4$, $m\|n$	$\frac{p^m+1}{2}$	[7]
odd	$p^{2k} - p^k + 1$	$\frac{n}{e}$ odd, $e = \gcd(n,k)$	$p^e + 1$	[12, 21]
odd	$p^n - 3$	any n	≤ 5	[16, 20]
5	$\frac{5^n-3}{2}$	any n	4 or 5	[19]
odd	$2p^{\frac{n}{2}} - 1$	n is even	$p^{\frac{n}{2}}$	This paper

2 The differential spectrum of $F(x) = x^{2q-1}$ over GF(q^2)

This section is devoted to study the differential spectrum of $F(x) = x^{2q-1}$ over GF(q^2), where q is an odd prime power. Before we investigate the differential spectrum of F, a useful lemma will be introduced first. For any $x \in \mathrm{GF}(q^2)^*$, if there exist $y \in \mathrm{GF}(q^2)^*$ such that $y^2 = x$, we call x a square element in GF(q^2). Otherwise, we call x a nonsquare element in GF(q^2). We have the following observation.

Lemma 2 Define $\mathbb{U} = \{z \in \mathrm{GF}(q^2) \mid z^{q+1} = 1\}$. For any square element $x \in \mathrm{GF}(q^2)^*$, there exist exactly two pairs, namely (y,z) and $(-y,-z)$, such that $x = yz = (-y)(-z)$, $\pm\, y \in \mathrm{GF}(q)^*$ and $\pm z \in \mathbb{U}$.

Proof Let ϵ be a primitive element in GF(q^2). Since x is a square, then $x = \epsilon^{2u}$ for some integer u in the range $0 \le u \le \frac{q^2-3}{2}$. Note that $(q+1, q-1) = 2$, then there exist integers s and t such that $s(q+1) + t(q-1) = 2$. Then

$$x = \epsilon^{2u} = \epsilon^{(s(q+1)+t(q-1))u} = \epsilon^{su(q+1)}\epsilon^{tu(q-1)}.$$

Put $y = \epsilon^{su(q+1)}$ and $z = \epsilon^{tu(q-1)}$, it can be checked that $y \in \mathrm{GF}(q)^*$ and $z \in \mathbb{U}$. Moreover, if there exist $y' \neq y$ and $z' \neq z$, such that $x = y'z'$, $y' \in \mathrm{GF}(q)^*$ and $z' \in \mathbb{U}$, then we have

$$\frac{y'}{y} = \frac{z}{z'} \in \mathbb{U}.$$

We conclude that $y' = -y$ since $\mathrm{GF}(q) \cap \mathbb{U} = \{\pm 1\}$. The desired result follows.

To determine the differential spectrum of F, we mainly study the derivative equation

$$(x+1)^{2q-1} - x^{2q-1} = b \tag{2}$$

for some $b \in \mathrm{GF}(q^2)$. Denote by $\delta(b)$ the number of solutions of (2) in GF(q^2). We have the following lemma.

Lemma 3 With the notation introduced above, we have

(i) $\delta(1) = q$,
(ii) $\delta(b)$ is either 0 or 2 for $b \neq 1$.

Proof When $b = 1$, (2) becomes

$$(x+1)^{2q-1} - x^{2q-1} = 1. \tag{3}$$

It is obvious that $x = 0$ and $x = -1$ are both solutions of (3). Now we assume that $x \neq 0, -1$. The (3) becomes

$$x(x+1)^{2q} - (x+1)x^{2q} = x(x+1),$$

then

$$x(x^q+1)^2 - (x+1)x^{2q} = x(x+1),$$

i.e.,

$$(x^q - x)^2 = 0.$$

We assert that x is a solution of (3) if and only if $x \in \mathrm{GF}(q)$. Hence $\delta(1) = q$.

Note that $2q - 1$ is odd, then the solutions of (2) come in pairs, i.e., x is a solution of (2) if and only if $-x-1$ is a solution of (2). Hence the value of $\delta(b)$ is even except when $x = -x - 1$, i.e., $x = -\frac{1}{2}$. In this latter case, the corresponding b equals to 1 since $-\frac{1}{2} \in \mathrm{GF}(q)$. Thus $\delta(b)$ is even for $b \neq 1$. In the rest of this proof, we will show $\delta(b) \leq 2$, for $b \neq 1$. If $b \neq 1$, then $x \neq 0$. We discuss the solutions of (2) in the following two disjoint cases.

Case 1 x is a square element in $\mathrm{GF}(q^2)^*$.

By Lemma 2, there exist $y \in \mathrm{GF}(q)^*$ and $z \in \mathbb{U}$ such that $x = yz$. Then (2) becomes

$$(yz + 1)^{2q-1} - (yz)^{2q-1} = b.$$

Note that $y^q = y$ and $z^q = z^{-1}$, we obtain

$$y(bz - 2z^{-1} + z^{-3}) = 1 - b. \tag{4}$$

Raising both sides of (4) into the power q, we have

$$y(b^q z^{-1} - 2z + z^3) = 1 - b^q. \tag{5}$$

The (4) and (5) lead to

$$(bz - 2z^{-1} + z^{-3})(1 - b^q) - (b^q z^{-1} - 2z + z^3)(1 - b) = 0,$$

which can be rewritten as

$$(z - z^{-1})\big((1-b)z^2 - (1 - b^{q+1}) + (1 - b^q)z^{-2}\big) = 0. \tag{6}$$

Note that $z - z^{-1} \neq 0$. Otherwise, $z = \pm 1$, then $x = yz \in \mathrm{GF}(q)$, which leads to $b = 1$, a contradiction. We then conclude that

$$(1-b)z^2 - (1 - b^{q+1}) + (1 - b^q)z^{-2} = 0. \tag{7}$$

Multiplying both sides of (7) by z^2 and denoting z^2 by u, we obtain

$$(1-b)u^2 - (1 - b^{q+1})u + (1 - b^q) = 0, \tag{8}$$

which is a quadratic equation of u. There exist at most two u's for a given $b \neq 1$. Moreover, from (4) we obtain

$$x = yz = \frac{1-b}{b - 2z^{-2} + z^{-4}} = \frac{1-b}{b - 2u^{-1} + u^{-2}}, \tag{9}$$

which means x is uniquely determined by u. Recall that $x = yz = (-y)(-z)$, z and $-z$ correspond to the same u. We conclude that (2) has at most two solutions in this case.

Case 2 x is a nonsquare element in $\mathrm{GF}(q^2)$.

Let ϵ be a primitive element in $\mathrm{GF}(q^2)$, let

$$\lambda = \begin{cases} \epsilon^{\frac{q+1}{2}}, & \text{if q } \equiv 1(\text{mod } 4), \\ \epsilon^{\frac{q-1}{2}}, & \text{if q } \equiv 3(\text{mod } 4). \end{cases}$$

Obviously, λ is a nonsquare element in $\mathrm{GF}(q^2)^*$. Moreover, if $q \equiv 1 (\mathrm{mod}\ 4)$, we have $\lambda^q = -\lambda$. If $q \equiv 3 (\mathrm{mod}\ 4)$, we have $\lambda^q = -\lambda^{-1}$.

Subcase 2.1. $q \equiv 1 (\mathrm{mod}\ 4)$.

Since x is a nonsquare element, then $x\lambda^{-1}$ is a square element. By Lemma 2, there exist $y \in \mathrm{GF}(q)^*$ and $z \in \mathbb{U}$ such that $x\lambda^{-1} = yz$, i.e., $x = \lambda yz$. The (2) becomes

$$\lambda y(bz + 2z^{-1} + z^{-3}) = 1 - b. \tag{10}$$

Raising both sides of (10) into the power q, we have

$$-\lambda y(b^q z^{-1} + 2z + z^3) = 1 - b^q. \tag{11}$$

The (10) and (11) lead to

$$(z + z^{-1})\big((1-b)z^2 + (1 - b^{q+1}) + (1 - b^q)z^{-2}\big) = 0 \tag{12}$$

If $z + z^{-1} = 0$, then $z^{-1} = -z$, we have $(\lambda z)^q = (-\lambda)(-z) = \lambda z$, i.e., $\lambda z \in \mathrm{GF}(q)$. Therefore, $x = \lambda z \cdot y \in \mathrm{GF}(q)$, which indicates $b = 1$, a contradiction. We assert that $z + z^{-1} \neq 0$, then the following identity holds.

$$(1-b)z^2 + (1 - b^{q+1}) + (1 - b^q)z^{-2} = 0. \tag{13}$$

Let $u = z^2$, then (13) becomes

$$(1-b)u^2 + (1 - b^{q+1})u + (1 - b^q) = 0, \tag{14}$$

which is a quadratic equation of u. There exist at most two u's for a given $b \neq 1$. Moreover, from (10) we obtain

$$x = \lambda yz = \frac{1-b}{b + 2z^{-2} + z^{-4}} = \frac{1-b}{b + 2u^{-1} + u^{-2}}, \tag{15}$$

which means x is uniquely determined by u. Recall that $x = \lambda yz = \lambda(-y)(-z)$, z and $-z$ correspond to the same u. We conclude that (2) has at most two solutions in this subcase.

Subcase 2.2. $q \equiv 3 (\mathrm{mod}\ 4)$.

Note that $\lambda^q = -\lambda^{-1}$ in this subcase. Similar to Subcase 2.1, there also exist $y \in \mathrm{GF}(q)^*$ and $z \in \mathbb{U}$ such that $x = \lambda yz$. Then (2) becomes

$$y(\lambda^{-3}z^{-3} + 2\lambda^{-1}z^{-1} + b\lambda z) = 1 - b. \tag{16}$$

Raising both sides of (16) into the power q, we have

$$y(-\lambda^3 z^3 - 2\lambda z - b^q \lambda^{-1} z^{-1}) = 1 - b^q. \tag{17}$$

The (16) and (17) lead to

$$(\lambda z + \lambda^{-1}z^{-1})\big((1-b)\lambda^2 z^2 + (1 - b^{q+1}) + (1 - b^q)\lambda^{-2}z^{-2}\big) = 0. \tag{18}$$

If $\lambda z + \lambda^{-1}z^{-1} = 0$, then $\lambda z = -\lambda^{-1}z^{-1} = \lambda^q z^q$, which means $\lambda z \in \mathrm{GF}(q)$. We have $x = \lambda yz \in \mathrm{GF}(q)$ and then $b = 1$, which is a contradiction. Thus we conclude that

$$(1-b)\lambda^2 z^2 + (1 - b^{q+1}) + (1 - b^q)\lambda^{-2}z^{-2} = 0. \tag{19}$$

Let $u = \lambda^2 z^2$, (19) becomes

$$(1-b)u^2 + (1-b^{q+1})u + (1-b^q) = 0, \tag{20}$$

which is a quadratic equation of u. Note that (14) and (20) are the same. There exist at most two u's for a given $b \neq 1$. Moreover, from (16) we obtain

$$x = \lambda yz = \frac{1-b}{b + 2\lambda^{-2}z^{-2} + \lambda^{-4}z^{-4}} = \frac{1-b}{b + 2u^{-1} + u^{-2}}, \tag{21}$$

which means x is uniquely determined by u. Recall that $x = \lambda yz = \lambda(-y)(-z)$, z and $-z$ correspond to the same u. We conclude that (2) has at most two solutions in this subcase (Table 2).

In the following, we will show that $\delta(b) \neq 4$ for $b \neq 1$. Otherwise, if $\delta(b) = 4$, (2) has two square solutions and two nonsquare solutions. The square solutions are

$$x_i = \frac{1-b}{b - 2u_i^{-1} + u_i^{-2}}, i = 1, 2,$$

where u_1 and u_2 are the two roots of the quadratic (8). Moreover, it can be easily seen that the roots of (14) and (20) are $-u_1$ and $-u_2$. Then by (15) and (21), the nonsquare solutions of (2) are

$$\frac{1-b}{b + 2(-u_i)^{-1} + (-u_i)^{-2}} = \frac{1-b}{b - 2u_i^{-1} + u_i^{-2}} = x_i, i = 1, 2,$$

which is a contradiction. Hence, (2) cannot have four solutions, i.e., $\delta(b) = 0$ or 2 for $b \neq 1$ since $\delta(b)$ is even. We complete the proof. □

By Lemma 3, the nonzero elements in the differential spectrum of F are ω_0, ω_2 and ω_q. We determine the differential spectrum of F in the following theorem.

Theorem 1 Let q be an odd prime power. Let $F(x) = x^{2q-1}$ be a power mapping defined over GF(q^2). The differential spectrum of F is given by

$$\mathbb{S} = \{\omega_0 = \frac{q^2+q-2}{2}, \omega_2 = \frac{q^2-q}{2}, \omega_q = 1\}.$$

Proof From Lemma 3 and (1), we obtain the following system of equations.

$$\begin{cases} \omega_0 + \omega_2 + \omega_q = q^2, \\ 2\,\omega_2 + q\,\omega_q = q^2, \\ \omega_q = 1. \end{cases}$$

Table 2 Possible solutions of the (2) for a given $b \neq 1$

Cases	Limitation of u	Solution x
Case 1	$(1-b)u^2 - (1-b^{q+1})u + (1-b^q) = 0$, (8)	$x = \frac{1-b}{b-2u^{-1}+u^{-2}}$
Subcase 2.1	$(1-b)u^2 + (1-b^{q+1})u + (1-b^q) = 0$, (14)	$x = \frac{1-b}{b+2u^{-1}+u^{-2}}$
Subcase 2.2	$(1-b)u^2 + (1-b^{q+1})u + (1-b^q) = 0$, (20)	$x = \frac{1-b}{b+2u^{-1}+u^{-2}}$

Solving the previous system of equations, we obtain the differential spectrum of F.

By Theorem 1 and Lemma 1, one can immediately deduce the following corollary.

Corollary 1 Let q be an odd prime power and $\mathrm{GF}(q^2)$ be the finite field with q^2 element. The number of solutions $(x_1, x_2, x_3, x_4) \in (\mathrm{GF}(q^2))^4$ of the system of equations

$$\begin{cases} x_1 - x_2 + x_3 - x_4 = 0, \\ x_1^d - x_2^d + x_3^d - x_4^d = 0 \end{cases}$$

is $4q^4 - 2q^3 - 3q^2 + 2q$, where $d = 2q - 1$.

3 Concluding remarks

Let $F(x) = x^{2q-1}$ be a power mapping over $\mathrm{GF}(q^2)$, where $2q - 1$ is a Niho exponent. When q is a power of 2, the differential spectrum of F was computed in [3]. In this paper, we studied the differential spectrum of F when q is an odd prime power. The differential spectrum of F was determined, and the number of solutions of a related system of equations followed. The application of the differential spectrum of F in sequence design, coding theory and combinatorial design is of great significance.

Acknowledgments The authors are very grateful to the anonymous reviewers for their comments and suggestions which improved the presentation and quality of this paper. H. Yan's research was supported by the National Natural Science Foundation of China (Grant No.11801468) and the Fundamental Research Funds for the Central Universities of China (Grant No.2682021ZTPY076).

References

1. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptology **4**(1), 3–72 (1991)
2. Blondeau, C., Canteaut, A., Charpin, P.: Differential properties of power functions. Int. J. Inf. Coding Theory **1**(2), 149–170 (2010)
3. Blondeau, C., Canteaut, A., Charpin, P.: Differential properties of $x \mapsto x^{2^t-1}$. IEEE Trans. Inf. Theory **57**(12), 8127–8137 (2011)
4. Blondeau, C., Perrin, L.: More differentially 6-uniform power functions. Des. Codes Cryptogr. **73**(2), 487–505 (2014)
5. Budaghyan, L.: Construction and Analysis of Cryptographic Functions. Springer-Verlag, New York (2014)
6. Carlet, C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, Cambridge (2021)
7. Choi, S.T., Hong, S., No, J.S., Chung, H.: Differential spectrum of some power functions in odd prime characteristic. Finite Fields and Appl **21**, 11–29 (2013)
8. Dempwolff, U.: CCZ equivalence of power functions. Des. Codes Cryptogr. **86**, 665–692 (2018)
9. Dobbertin, H., Helleseth, T., Kumar, P.V., Martinsen, H.: Ternary m-sequences with three-valued cross-correlation function : new decimations of Welch and Niho type. IEEE Trans. Inf. Theory **47**(4), 1473–1481 (2001)
10. Helleseth, T.: Some results about the cross-correlation function between two maximal linear sequences. Discrete Math **16**(3), 209–232 (1976)
11. Helleseth, T., Rong, C., Sandberg, D.: New families of almost perfect nonlinear power mappings. IEEE Trans. Inf. Theory **45**(2), 475–485 (1999)

12. Lei, L., Ren, W.L., Fan, C.L.: The differential spectrum of a class of power functions over finite fields. Adv. Math. Commun. **15**(3), 525–537 (2021)
13. Li, N., Zeng, X.Y.: A survey on the applications of Niho exponents. Cryptogr. Commun. **11**(3), 509–548 (2019)
14. Niho, Y.: Multivalued cross-correlation functions between two maximal linear recursive sequence. PhD thesis, Univ. of Southern California, Los Angle (1972)
15. Nyberg, K.: Differentially uniform mappings for cryptography. Advances in Cryptology–EUROCRYPT'93, Lecture Notes in Computer Science **765**, 55–64 (1994)
16. Xia, Y.B., Zhang, X.L., Li, C.L., Helleseth, T.: The differential spectrum of a ternary power mapping. Finite Fields and Appl **64** (2020)
17. Xiong, M.S., Yan, H.D.: A note on the differential spectrum of a 4-uniform power function. Finite Fields and Appl **48**, 117–125 (2017)
18. Xiong, M.S., Yan, H.D., Yuan, P.Z.: On a conjecture of differentially 8-uniform power function. Des. Codes Cryptogr **86**(6), 1601–1621 (2018)
19. Yan, H.D., Li, C.J.: Differential spectra of a class of power permutations with characteristic 5. Des. Codes Cryptogr. **89**(6), 1181–1191 (2021)
20. Yan, H.D., Xia, Y.B., Li, C.L., Helleseth, T., Xiong, M.S., Luo, J.Q.: The differential spectrum of the power mapping x^{p^n-3}. IEEE Trans. Inf. Theory (2021). https://doi.org/10.1109/TIT.2022.3162334
21. Yan, H.D., Zhou, Z.C., Weng, J., Wen, J.M., Helleseth, T., Wang, Q.: Differential spectrum of kasami power permutations over odd characteristic finite fields. IEEE Trans. Inf. Theory **65**(10), 6819–6826 (2019)